A PARADIGM SHIFT TO OPTIMIZE THE DIGITAL FORENSICS PROCESS

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna University

by

Barkhashree
2K19-PFE-004

Under the supervision of

Dr. Parneeta Dhaliwal
Professor

Department of Computer Science and Technology
Faculty of Engineering

MANAV RACHNA
vidyanatariksha
MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

Year 2021

MANAV RACHNA
Vidyanatariksha

MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

Date: 29.10.2021

DECLARATION BY THE SCHOLAR

I hereby declare that the short synopsis in the area of "A Paradigm Shift to Optimize the Digital Forensics Process" being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in department of Computer Science and Technology under Faculty of Engineering of Manav Rachna University, Faridabad during the academic year 2020-2021.

It is the work that is expected to be carried out under the supervision of Dr. Parneeta Dhaliwal. Further, it is certified that short synopsis is within the plagiarism limit and copy of the same is attached as per University norms.

(Barkhashree)
2K19-PFE-004

Dr. Parneeta Dhaliwal,
Professor, Faculty of Engineering

ABSTRACT

The explosion of digital technology in today's world provides some unique opportunities towards creating a modern society but it can also be abused and misused by individuals. The technology driven society entices criminals to carry out digital crimes through the use of internet or information communication technology. These digital platforms must be examined for the identification and analysis of any digital evidence stored on them. Digital Forensics (DF) aims to investigate a criminal activity by a thorough inspection of the digital evidence and bring the perpetrators to justice. Current research in Digital Forensics has highlighted that apart from probing of digital evidence, integrating a study of the behaviour of the offender and the victim through Behavioural Evidence Analysis (BEA) is important for an effectual forensic investigation. Although the analysis of behavioural clues in DF proceedings has gained attention but its adoption within the investigation process is limited. This study performs a review of the existing DF approaches that comprise behavioural analysis. The research also proposes a homogenous approach to analysis of behaviour clues during Digital Forensics investigations. The study further attempts to contribute to a more scientifically sound DF process by developing a behavioural digital forensics approach that includes the unexplored characteristics of the forensic domain in question. Additionally, the research aims to study Machine Learning (ML) techniques and incorporate it in behavioural digital forensics.

Key words: Digital Forensics, Forensic Analysis, Digital Evidence, Criminal Profiling, Behavioural Analysis

CONTENTS

S. No.	Description	Page No.
1	Introduction	1-4
2	Literature Review	5-10
3	Description of Broad Area	11
4	Objectives of the Study	12
5	Methodology to be adopted	13
6	Expected Outcome of the Research	14
7	References	15-21

1. INTRODUCTION

The role of technology is ever-increasing in today's world. The proliferation of digital technology has impacted the lifestyle of the masses but it also has had a tremendous effect on their behaviour (Holt, Bossler, & Seigfried-Spellar, 2017; Holt et al., 2018b). Furthermore, the easily accessible tools and technology make it mandatory to determine the constructive and destructive impacts that it leaves on society. The inception of technology has undoubtedly provided some unique opportunities (Sedera & Cooper, 2019) towards creating a modern society but it can also be abused and misused by individuals. The plethora of tools and technologies available today that allow criminal acts to occur anywhere in the world serve as an incentive for criminals. The anonymity offered by the internet has led to an upsurge in the number of crimes involving computers and cybernetics (MacDermott, Baker, Buck, Iqbal, & Shi, 2020).

The offenses carried out by criminals facilitated by a computer (McMurdie, 2016), computer networks or any other type of information communications technology are known as Digital crimes. It also involves classic crimes (such as murder, blackmailing, kidnaping, defamation), that misuse technological adeptness and accessibility to information. Digital crimes encompass several criminal acts like hacking, damage to computer resources, disruption of networks, malware attacks, money related frauds, information theft, identity theft, cyber vandalism, denial of service, copyright violation, piracy and child pornography. The motivation behind these crimes may involve subjects that are personal, commercial, political, anarchical, or other, however, the rudimentary attack and intrusion techniques generally remain identical. The impact of globalization and cyber developments is such that the digital crimes perpetrated at both local and global level is increasing. The incessantly increasing complexity of digital crimes exhibit both the enhanced complexity of our digital technology and services mix, in addition to ongoing advancements in security (MacDermott et al., 2020). This may pose new challenges to gather evidence in case of digitally committed crimes and their successful resolution.

Formerly, criminal investigations revolved around the examination of procured evidence from the place of crime. Whereas today, in the digital era, the evidence to assay is in digital or electronic form (Macdermott, Baker, & Shi, 2018) and is called Digital Evidence. Digital evidence is any information related to the crime that is stored or transmitted in digital form. It may comprise of computer-generated log files, browsing history, or metadata and may be accrued from computer systems, smart digital devices, or network traffic. The proliferation of digital crimes presents an essential investigative challenge vis-à-vis the review of evidence residing on the mass of devices that can be exploited for perpetrating a crime. The comprehensive probing of digital evidence can establish the occurrence of any online or offline criminal activity. Thus, there is a need for an investigation process that examines digital information in the form of digital evidence and identify the involved suspects, determines motivations and behaviour, and depicts a chronology of the crime events (Al Mutawa, Bryce, Franqueira, Marrington, & Read, 2019).

The mechanism required to obtain and analyze digital evidence to solve criminal cases is called Digital Forensics (Årnes, 2017; Sammons, 2015). It is a new and fast-growing form of investigative practice wherein the forensic specialists use modern forensic software tools to capture and examine digital evidence. The framework for the DF process includes the stages of evidence collection/acquisition, examination, analysis and lastly report generation (Hassan & Hassan, 2019). During the collection/acquisition phase (Varol & Sönmez, 2017b), all devices of interest toward uncovering digital evidence are captured from the crime scene and data preservation is undertaken to retain the authenticity of evidence. The examination phase (Holt et al., 2018a) of digital forensics investigation, is concerned with the recovery or extraction of digital data from electronic devices. The analysis phase (Varol & Sönmez, 2017a) employs state-of-the-art technology, tools and sophisticated software to yield substantial results in identifying the perpetrator of the crime and setting out the timeline of occurrences. The report thus generated must be accurate, precise and its integrity must be established before presenting it in the court of law. Digital forensics practices (Sammons, 2015) must also be assured by quality assurance measures for investigatory standards. As the technological complexity and storage capabilities of digital devices is increasing

(Rahman & N. A. Khan, 2016), the forensic digital investigations call for a more sophisticated and comprehensive approach for the capture and inspection of digital evidence (Holt et al., 2018a; MacDermott et al., 2020).

Experts in digital forensic investigation are facing unseen challenges due to the new, advanced technologies, used in digital devices, and adopted by criminals alike. The difficulties can be overcome through a hybrid digital forensic task process (Rahman & N. A. Khan, 2016) that incorporates other dimensions like behavioural clues of the offender into the traditional DF process. For instance, in forensic criminal investigations, the behavioural mannerisms of the actors involved in a crime can be done through a process called Behavioural Evidence Analysis (Turvey, 2016; Turvey & Esparza, 2016). It involves the discovery and examination of behavioural clues of the offender and the victim from the digital evidence. Behavioural Evidence Analysis considers a deductive, case-based exploratory approach to forensic criminal investigations. It inspects particular criminal cases to detect specific behavioural or personal traits of the suspect. BEA involves four types of analysis (Turvey, 2016) comprising equivocal forensic analysis (Al Mutawa, Bryce, Franqueira, & Marrington, 2015), forensic victimology (Petherick, 2019; Petherick & Ferguson, 2015), identification of crime scene characteristics (Almond, McManus, Giles, & Houston, 2017; Wang et al., 2018) and identification of offender traits (Turvey, 2012).

The first step includes analyzing the available evidence to determine offense behaviour. This forms a core concept of the BEA investigative process and is strongly recommended by practitioners and researchers to reach correct conclusions. It advocates to thoroughly and objectively examine all evidence, without bias or assumptions. The second step of forensic victimology comprehends the role of the victim in the crime. It deals with finding out the specific traits of victim's lifestyle and mannerisms that led to his selection, assessing the risk exposure of victim to the crime. The third step involves crime scene examination to reveal the choices undertaken by the offender in relation to the offense (signature ways and modus operandi). It implicates finding hidden aspects of crime scene which can uncover further evidence to define behavioural attributes of the suspects more clearly. In the last stage, behavioural traits of the suspect are specified based on offender characteristics revealed in preceding stages. The discovered

behavioural characteristics of the offender are to be used in conjunction with the DF investigation process to provide a more coherent reconstruction of the crime.

The incorporation of Behavioural Analysis into the DF process enhances the quality (Al Mutawa et al., 2019) of the results yielded by the DF process. Forensic processes (Sammons, 2015) must be collaborated with the cognitive and human aspects to enrich it, so it proves to be a more efficient and comprehensive evaluation that considers other facets like human behavioural and psychological elements. The inclusion of elements of behaviour into the digital forensics process can provide a new direction to forensic analysis and investigations. It can aid the study of Digital Forensics across varied domains including, but not limited to, social network analysis, web content analysis, social media analysis, digital footprints analysis, digital content analysis, crime detection in several areas such as, finance, online forums, network interactions, web communications etc. The existing literature offers a customary description of the incorporation of behaviour analysis techniques in digital forensic investigations. Owing to its recognized efficacy, the implementation of behaviour-based approaches in digital forensics need to be studied and researched.

With huge digital information available from various sources, it is often a challenge to find useful data for furthering the forensic investigation. Data mining and Machine Learning provide effective and efficient tools that allow for the easy processing and utilization of the online data. Machine Learning is an ever-evolving field with newer and enhanced algorithms. ML algorithms can be used to push the envelope even further about speed, space and accuracy parameters.

As the digital investigations pose fresh challenges, further research is required on how behavioural DF methods can be made faster by using Machine Learning technologies. It can be noteworthy to ascertain how to direct the forensic process to include behavioural pointers and to understand what contribution can be harnessed from ML techniques under such circumstances.

2. LITERATURE REVIEW

This section presents the survey of the existing work on behavioural analysis, digital forensics process models and existing behavioural Digital Forensics methods that incorporate human factors in a DF investigation.

The consideration of behavioural physiognomies while probing crimes has been emphasized in several studies. Bryant (Bryant, 2016) pointed out that criminology can prove effective in investigating digital crimes. The application can aid investigators by giving pointers and leads and access to a wealth of information. Kaati et al. (Kaati, Shrestha, & Sardella, 2016) argued that the psychological state of the criminal and his tendency of committing an offense can be deciphered from their spoken or written language for example, threat notes or verbal linguistics.

Tonkin et al. (Tonkin et al., 2017) used a dataset of serial sexual assaults from five countries comprising 3,364 cases. He employed various statistical procedures to examine offender behaviour. The results revealed that patterns of offender behaviour could be established vis-à-vis the modus operandi, extent of involved violence or victim restraint techniques. This also successfully linked sexual crimes carried out by the same offender. Beauregard et al. (Beauregard, Busina, & Healey, 2017) conducted studies on 624 convicted sexual criminals and their associated case files. Based on the probability of confession in an interrogation, five profiles each for the offender and the victim were identified. It has helped in designing interrogation strategies for every profile to obtain criminal confessions.

Rogers (M. Rogers, 2003) in his research described the efficacy of behavioural analysis in the digital crime investigation process. He argued that both conventional and digital crimes essentially follow similar procedures for investigation: inspecting events of crime, offender motivations, and modus operandi. Lowe (Eagle & 2002, n.d.) emphasized on the study of criminal behaviour in cases of crimes against persons, property, gang crimes and so on. This research focused on examining the role of criminal profiling in the operational phase of an investigation. Bennett and Hess (Bennett, Learning, & 2007, n.d.) analyzed a variety of crimes like sex offenses, crimes against children, robbery, drug abuse, computer crimes and so on. They provided details on developing the suspect's

traits based on the modus operandi information, psychological profiling, geographic profiling, and racial profiling.

The inexorable evolution of technology has increased the number and complexity of cybercrimes (Lillis, Becker, O'Sullivan, & Scanlon, 2016). Due to this, numerous challenges have arisen in the digital forensics sphere (Vincze, 2016). These may be related to difficulties in law enforcement, technical complications, lack of expertise among investigating personnel and absence of standardized DF procedures (Karie & Venter, 2015). This suggests a need for the development of inventive techniques (Ch, Gadekallu, Abidi, & Al-Ahmari, 2020) and methodologies over conventional ones for probing digital offenses.

An Abstract DF Model (Reith, Carr, & Gunsch, 2002) was developed that was not dependent on specific technologies. It had nine stages, including, identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence. A drawback of this model was that it was too general for practical use and its testing and validation was difficult.

An Integrated Digital Investigation Model consisting of same number of stages for the digital and physical crime scenes was proposed by Carrier and Spafford (Carrier & Spafford, 2003). It contained five groups further elaborating into 17 phases. The groups included readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review. The practical applicability of this model was not established in real cases.

Enhanced Digital Investigation Model (Baryamureeba & Tushabe, n.d.) was a modification of the Integrated Digital Investigation model that split the investigation into physical and primary (digital) crime scenes. This system had five steps, namely, readiness, deployment, trace back, dynamite, and review. This model was later found to be useful only in investigation of digital frauds (Mir, Shoaib, & Shahzad Sarfraz, n.d.).

Beebe and Clark (Beebe & Clark, 2005) presented a multi-tiered DF framework called Hierarchical Objective-based Model. The first tier consisted of six stages, namely, preparation, incident response, data collection, data analysis, presentation of findings, and incident closure. The second tier included task hierarchies and objectives-based

subphases. This approach was tested on fictional cases and provided no detailed explanation of levels other than analysis stage.

Perumal (Perumal, 2009) claimed that no DFIPM developed previously focused on the full scope of investigation and only stressed on specific aspects. He presented a model that comprised seven stages including identification, planning, reconnaissance, analysis, results, proof and defense, and the diffusion of information. However, this model did not stand up to its claims and only focused on acquisition of different kinds of digital evidence. Another drawback was the feasibility of its implementation to real life scenarios.

Cohen (Cohen, 2010) developed a DF model that concentrated primarily on the examination stage of investigation (analysis, interpretation, attribution, reconstruction). This process model addressed the legal challenges relating to digital evidence, but its practical realization was not demonstrated.

Agarwal et al. (Agarwal & Gupta, n.d.) designed the Systematic Digital Forensic Model for handling static and volatile digital evidence. This scheme had 11 phases, viz. (1) preparation, (2) securing the scene, (3) survey and recognition, (4) documentation of the scene, (5) communication shielding, (6) evidence collection, (7) preservation, (8) examination, (9) analysis, (10) presentation, and (11) result. The applicability of this design was restricted to digital fraud and cybercrimes.

Ademu et al. (Ademu, Imafidon, & Preston, 2011) proposed an iterative multitiered model for DF investigation where each phase included various subphases. The four tiers were identified as preparation, interaction, reconstruction, and presentation. This model inherited its structure from previous DF models but did not portray a detail of the phases and subphases. Its real-world applicability has also not been tested.

Kohn et al. (Kohn, Eloff, & Eloff, 2013) crafted an integrated DF model that consisted of six phases and many subphases. In this, documentation was recognized as an incessant process to be executed during all phases of investigation. The phases constituted preparation, incident, incident response, digital forensics investigation, physical investigation and presentation. However, the applicability of this model was limited to organizational crimes.

Montasari et al. (Montasari, Peltola, & Evans, 2015) proposed an eight-stage DF model involving readiness, identification, incident response, collection, examination, analysis, presentation, and incident closure. The authors did not provide a detailed description of each phase and hence this model was of very little use to DF practitioners.

Karie et al. (Karie, Kebande, & Venter, 2019) presented a DF model that identified five stages, namely, (1) initialization, (2) data sources identification, (3) application of deep learning (DL) methods, (4) forensic reporting/presentation, and (5) decision making and case closure. This structure focuses on evidence which is the most important and diverse part of DF. An important advantage of using this methodology is that machine learning (Gadekallu et al., 2020) can be implemented in each of its stages. However, the implementation of this design varies depending on the type of evidence.

These digital forensic process models discussed so far disregard the social, motivational or behavioural scopes of criminal actions that play a major role in recognizing probable evidence during the investigation. There was no process model developed until 2014 that accredited the efficacy of involving behavioural analysis within the DF investigations. However, the need for integrating behavioural clues of involved parties in criminal forensic investigations has been realized by researchers lately. There is very limited study in incorporating BEA in an investigation of digital crimes. There exists even lesser literature that describes the utility of behavioural analysis to construe digital evidence in these cases.

Silde and Angelopoulou (Silde & Angelopoulou, 2014) proposed a Cyberstalker profiling methodology by integrating BEA into a traditional DF investigation framework. This model involved the stages of discovery/accusation, examination, and analysis. Discovery step is the survey phase where assessment of the devices of interest is done. The examination stage consists of evidence search and acquisition, storage, recovery and preservation. Finally, the analysis comprises organization, in-depth review, and reconstruction of evidence.

Mutawa et al. (Al Mutawa et al., 2019) proposed a BEA DF model that included phases of review, recognition and collection, examination and analysis, and interpretation and reporting. The initial stage of review deals with available evidence and observes potential offender motivations, behaviour, and crime scene characteristics. It

encompasses contextualization and classification of case as well as prioritization of evidence. The recognition step identifies the authorship of the evidence files stored in digital devices. The third stage comprises of examining and analyzing acquired information to derive answers to all investigation questions. The final step attempts to reconstruct the crime based on results of analysis in previous stages. This would then be used to build a comprehensive report.

Rogers (M. K. Rogers, 2016) gave a behavioural Digital Forensics model that had six phases: (1) case classification, (2) context analysis, (3) data collection, (4) statistical analysis, (5) timeline analysis/visualization, and (6) decision/opinion. Here, first step of investigation is to decipher the category of the case in question for example, pornography, identity theft, extortion, homicide, etc. Next step is to understand the context of the underlying case. This lets the DF practitioners to narrow their search for evidence onto specific locations on the suspect's digital devices or social networks. Data collection is the acquisition of evidence and its storage such that it can be studied for associations, patterns and timeline analysis. The statistical analysis stage monitors the web browser history of the suspect to check the frequency of visited pages to reveal patterns of his/her online behaviour. The visualization of a timeline provides important information about the digital device's usage in case of multiple suspects. In the final step, an opinion has to be formed based on the results from each of the phases and determine the correct finding.

The increasing complexities and capabilities of digital technology has triggered the need for monitoring its use to prevent any abuse. Thus, the ways and methods of digital forensics must also advance to match the new face of digital proficiencies. Due to the huge and continuous real time digital data and evidence, simple forensic techniques may not always achieve desired success rate. As a result, researchers must also focus towards machine learning techniques which can provide a way to direct the incorporation of behaviour into the forensic procedures. For instance, a recent study discussed machine learning based approach for detection of suspicious social network profiles (Sahoo & Gupta, 2020). Other researches elaborate the use of ML algorithms for the detection of: Fraudulent user behaviour in water consumption (Gopal & Balaji, 2020), Suspicious user behavior in shoplifting cases (Martínez-Mascorro, Abreu-Pederzini, Ortiz-Bayliss, &

Terashima-Marín, 2020), Identity theft crimes using text mining (Nokhbeh Zaeem, Manoharan, Yang, & Barber, 2017), Hate speech on social media (Vijayaraghavan, Larochelle, & Roy, 2021), Use of abusive text (Eshan & Hasan, 2018), Illegal transactions on bitcoins (Lee, Maharjan, Ko, & Hong, 2020) and, Phishing websites (Ali, 2017) etc.

3. DESCRIPTION OF TOPIC

The study discusses the development of novel techniques in the digital forensics process. It emphasizes on the inclusion of behaviour into digital forensics to provide a new direction to forensic analysis and investigations.

It tries to incorporate behaviour in the field of digital forensics across various domains including, but not limited to, social network analysis, web content analysis, social media analysis, digital footprints analysis, digital content analysis, digital crime detection in several areas such as, finance, online forums, network interactions, web communications etc.

The research proposes behaviour-based approaches in digital forensics. It further tries to harness the contribution of technologies like Machine Learning to direct forensic analysis in such approaches.

4. OBJECTIVES OF RESEARCH

The main objectives of the research work are listed as below:

i. To perform a review of existing Behavioural Evidence Analysis approaches for Digital Forensics.

ii. To develop a homogenous BEA model for varied forensic domains.

iii. To develop a behavioural DF approach that includes the unexplored characteristics of the forensic domain in question.

iv. To develop a novel behavioural Digital Forensics model using Machine Learning.

5. METHODOLOGY TO BE ADOPTED

The following methodology will be adopted for the successful completion of the research work:

i. The existing literature corresponding to behavioural analysis in Digital Forensics to be studied to perform a comprehensive review of the existing BEA approaches for digital forensics, highlighting their advantages and limitations.

ii. Proposing a homogenous approach to BEA for Digital Forensics.

iii. Designing a behavioural DF model that includes the unexplored characteristics of the forensic domain in question.

iv. Machine learning techniques to be studied and its incorporation into behavioural Digital Forensics will be attempted.

6. EXPECTED OUTCOME OF RESEARCH

The outcome of the research undertaken is as below:

i. A review of existing behavioural analysis approaches for Digital Forensics process to reveal that there is more scope to application of behaviour analysis into the DF process. Behavioural analysis is a new direction in DF that can be aligned with the forensic processes to yield better results.

ii. Development of a homogenous Behavioural Evidence Analysis model for Digital Forensics.

iii. Design of a behavioural DF approach that includes unexplored characteristics of the forensic domain in question.

iv. Application of Machine Learning algorithms to behavioural Digital Forensics.

7. REFERENCES

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 2). Retrieved from www.ijacsa.thesai.org

Agarwal, A. A., & Gupta, M. M. (n.d.). Systematic Digital Forensic Investigation Model. In *Saurabh Gupta & Prof. (Dr.) S.C. Gupta International Journal of Computer Science and Security (IJCSS)*.

Al Mutawa, N., Bryce, J., Franqueira, V. N. L., & Marrington, A. (2015). Behavioural evidence analysis applied to digital forensics: An empirical analysis of child pornography cases using P2P networks. *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 293–302. https://doi.org/10.1109/ARES.2015.49

Al Mutawa, N., Bryce, J., Franqueira, V. N. L., Marrington, A., & Read, J. C. (2019). Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes. *Digital Investigation*, *28*, 70–82. https://doi.org/10.1016/j.diin.2018.12.003

Ali, W. (2017). Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection. *Article in International Journal of Advanced Computer Science and Applications*, *8*(9). https://doi.org/10.14569/IJACSA.2017.080910

Almond, L., McManus, M. A., Giles, S., & Houston, E. (2017). Female Sex Offenders: An Analysis of Crime Scene Behaviors. *Journal of Interpersonal Violence*, *32*(24), 3839–3860. https://doi.org/10.1177/0886260515603976

Årnes, A. (2017). Digital forensics. In *John Wiley & Sons*. Retrieved from https://books.google.nl/books?hl=en&lr=&id=xqNaDwAAQBAJ&oi=fnd&pg=PR15&dq=digital+forensics+what+is+it&ots=q5gNbii2bA&sig=5oytwpZxnnDTFe97xKBB95-BN34&redir_esc=y#v=onepage&q=digital forensics what is it&f=false

Baryamureeba, V., & Tushabe, F. (n.d.). *The Enhanced Digital Investigation Process Model*. Retrieved from www.makerere.ac.ug/ics

Beauregard, E., Busina, I., & Healey, J. (2017). Confessions of sex offenders: extracting offender and victim profiles for investigative interviewing. *Journal of Criminal Psychology*, *7*(1), 13–28. https://doi.org/10.1108/JCP-10-2016-0031

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147–167. https://doi.org/10.1016/j.diin.2005.04.002

Bennett, W., Learning, K. H.-C., & 2007, undefined. (n.d.). *Investigating violent crimes, in criminal investigation*.

Bryant, R. (2016). *Digital Crime*. 19–60. https://doi.org/10.4324/9781315601083-7

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. In *International Journal of Digital Evidence Fall* (Vol. 2). Retrieved from www.ijde.org

Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify Cyber Crime offenses using machine learning. *Sustainability (Switzerland)*, *12*(10), 4087. https://doi.org/10.3390/SU12104087

Cohen, F. (2010). Toward a science of digital forensic evidence examination. *IFIP Advances in Information and Communication Technology*, *337 AICT*, 17–35. https://doi.org/10.1007/978-3-642-15506-2_2

Eagle, A. L.-N. L., & 2002, undefined. (n.d.). *Criminal profiling in the investigative process*.

Eshan, S. C., & Hasan, M. S. (2018). An application of machine learning to detect abusive Bengali text. *20th International Conference of Computer and Information Technology, ICCIT 2017*, *2018-January*, 1–6. https://doi.org/10.1109/ICCITECHN.2017.8281787

Gadekallu, T. R., K, M. M., S, S. K., Kumar, N., Hakak, S., & Bhattacharya, S. (2020). *Blockchain based Attack Detection on Machine Learning Algorithms for IoT based E-Health Applications*. Retrieved from http://arxiv.org/abs/2011.01457

Gopal, G. V., & Balaji, V. (2020). Detection of Fraudulent Behaviour in Water Consumption using Machine Learning Algorithms. *Journal of Engineering Sciences*, 11(7), 399–406.

Hassan, N. A., & Hassan, N. A. (2019). Digital Forensics Report. In *Digital Forensics Basics* (pp. 323–326). https://doi.org/10.1007/978-1-4842-3838-7_11

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). Cybercrime and Digital Forensics. In *Cybercrime and Digital Forensics*. https://doi.org/10.4324/9781315296975

Holt, T. J., Bossler, A. M., Seigfried-Spellar, K. C., Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018a). Acquisition And Examination of Forensic Evidence. In *Cybercrime and Digital Forensics* (pp. 527–569). https://doi.org/10.4324/9781315296975-13

Holt, T. J., Bossler, A. M., Seigfried-Spellar, K. C., Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018b). Technology and Cybercrime. In *Cybercrime and Digital Forensics* (pp. 1–37). https://doi.org/10.4324/9781315296975-1

Iwendi, C., Jalil, Z., Javed, A. R., Thippa Reddy, G., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection against Cyber-Attacks. *IEEE Access*, *8*, 72650–72660. https://doi.org/10.1109/ACCESS.2020.2988160

Kaati, L., Shrestha, A., & Sardella, T. (2016). Identifying Warning Behaviors of Violent Lone Offenders in Written Communication. *IEEE International Conference on Data Mining Workshops, ICDMW*, *0*, 1053–1060. https://doi.org/10.1109/ICDMW.2016.0152

Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, *1*, 61–67. https://doi.org/10.1016/j.fsisyn.2019.03.006

Karie, N. M., & Venter, H. S. (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, *60*(4), 885–893. https://doi.org/10.1111/1556-4029.12809

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers and Security*, *38*, 103–115. https://doi.org/10.1016/j.cose.2013.05.001

Lee, C., Maharjan, S., Ko, K., & Hong, J. W. K. (2020). Toward Detecting Illegal Transactions on Bitcoin Using Machine-Learning Methods. *Communications in Computer and Information Science*, *1156 CCIS*, 520–533. https://doi.org/10.1007/978-981-15-2777-7_42

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). *Current Challenges and Future Research Areas for Digital Forensic Investigation*. Retrieved from http://arxiv.org/abs/1604.03850

MacDermott, Á., Baker, T., Buck, P., Iqbal, F., & Shi, Q. (2020). The internet of things: Challenges and considerations for cybercrime investigations and digital forensics. *International Journal of Digital Crime and Forensics*, *12*(1), 1–13. https://doi.org/10.4018/IJDCF.2020010101

Macdermott, Á., Baker, T., & Shi, Q. (2018). Iot Forensics: Challenges for the Ioa Era. *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, *2018-January*, 1–5. https://doi.org/10.1109/NTMS.2018.8328748

Martínez-Mascorro, G. A., Abreu-Pederzini, J. R., Ortiz-Bayliss, J. C., & Terashima-Marín, H. (2020). Suspicious Behavior Detection on Shoplifting Cases for Crime Prevention by Using 3D Convolutional Neural Networks. *Computation*, *9*(2), 24. https://doi.org/10.3390/computation9020024

McMurdie, C. (2016). The cybercrime landscape and our policing response. *Journal of Cyber Policy*, *1*(1), 85–93. https://doi.org/10.1080/23738871.2016.1168607

Mir, S. S., Shoaib, U., & Shahzad Sarfraz, M. (n.d.). *Analysis of Digital Forensic Investigation Models*. Retrieved from https://sites.google.com/site/ijcsis/

Montasari, R., Peltola, P., & Evans, D. (2015). Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. *Communications in Computer and Information Science*, *534*, 83–95. https://doi.org/10.1007/978-3-319-23276-8_8

Nokhbeh Zaeem, R., Manoharan, M., Yang, Y., & Barber, K. S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers and Security*, *65*, 50–63. https://doi.org/10.1016/j.cose.2016.11.002

Perumal, S. (2009). Digital Forensic Model Based On Malaysian Investigation Process. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 9).

Petherick, W. (2019). Forensic Victimology Assessments in Child Abuse and Neglect Cases. In *Child Abuse and Neglect* (pp. 135–149). https://doi.org/10.1016/b978-0-12-815344-4.00008-8

Petherick, W., & Ferguson, C. (2015). Forensic Victimology. In *Applied Crime Analysis* (pp. 62–80). https://doi.org/10.1016/B978-0-323-29460-7.00004-1

Rahman, S., & N. A. Khan, M. (2016). Digital Forensics through Application Behavior Analysis. *International Journal of Modern Education and Computer Science*, *8*(6), 50–56. https://doi.org/10.5815/ijmecs.2016.06.07

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. In *International Journal of Digital Evidence Fall* (Vol. 1). Retrieved from www.ijde.org

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers and Security*, *22*(4), 292–298. https://doi.org/10.1016/S0167-4048(03)00405-X

Rogers, M. K. (2016). Psychological profiling as an investigative tool for digital forensics. In *Digital Forensics: Threatscape and Best Practices* (pp. 45–58). https://doi.org/10.1016/B978-0-12-804526-8.00003-4

Sahoo, S. R., & Gupta, B. B. (2020). Fake profile detection in multimedia big data on

online social networks. *International Journal of Information and Computer Security*, *12*(2–3), 303–331. https://doi.org/10.1504/IJICS.2020.105181

Sammons, J. (2015). Digital Forensics: Threatscape and Best Practices. In *Digital Forensics: Threatscape and Best Practices*. https://doi.org/10.1016/C2014-0-01932-6

Sedera, D., & Cooper, V. (2019). *PANEL : Digital Transformation : Environmental friend or foe ?* 982–987.

Silde, A., & Angelopoulou, O. (2014). A digital forensics profiling methodology for the cyberstalker. *Proceedings - 2014 International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS 2014*, 445–450. https://doi.org/10.1109/INCoS.2014.118

Tonkin, M., Pakkanen, T., Sirén, J., Bennell, C., Woodhams, J., Burrell, A., … Santtila, P. (2017). Using offender crime scene behavior to link stranger sexual assaults: A comparison of three statistical approaches. *Journal of Criminal Justice*, *50*, 19–28. https://doi.org/10.1016/j.jcrimjus.2017.04.002

Turvey, B. E. (2012). *Criminal profiling : an introduction to behavioral evidence analysis*. Academic Press.

Turvey, B. E. (2016). Applied Criminal Profiling: An Introduction. In *Behavioral Evidence Analysis: International Forensic Practice and Protocols*. https://doi.org/10.1016/B978-0-12-800607-8.00001-X

Turvey, B. E., & Esparza, M. A. (2016). Behavioral Evidence Analysis: International Forensic Practice and Protocols. In *Behavioral Evidence Analysis: International Forensic Practice and Protocols*. https://doi.org/10.1016/C2013-0-15462-1

Varol, A., & Sönmez, Y. Ü. (2017a). Review of evidence analysis and reporting phases in digital forensics process. *2nd International Conference on Computer Science and Engineering, UBMK 2017*, 923–928. https://doi.org/10.1109/UBMK.2017.8093563

Varol, A., & Sönmez, Y. Ü. (2017b). Review of evidence collection and protection

phases in digital forensics process. *International Journal of Information Security Science*, 6(4), 39–46.

Vijayaraghavan, P., Larochelle, H., & Roy, D. (2021). *Interpretable Multi-Modal Hate Speech Detection*. Retrieved from http://arxiv.org/abs/2103.01616

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163

Wang, S., Wang, X., Ye, P., Yuan, Y., Liu, S., & Wang, F. Y. (2018). Parallel Crime Scene Analysis Based on ACP Approach. *IEEE Transactions on Computational Social Systems*, *5*(1), 244–255. https://doi.org/10.1109/TCSS.2017.2782008

MANAV RACHNA
vidyaantarikshah

Swami Vivekananda Library and Resource Centre
Manav Rachna University

SIMILARITY VERIFICATION CERTIFICATE

Title: A PARADIGM SHIFT TO OPTIMIZE THE DIGITAL FORENSICS PROCESS

Researcher: BARKHASHREE Registration Number: 2K19-PFE-004

Supervisor: DR. PARNEETA DHALIWAL Department: DEPTT. OF COMPUTER SC. AND TECHNOLOGY

This is to certify that the above mentioned Short ✓ Synopsis/~~Thesis~~ was scanned for similarity index through Turnitin Software on 27.10.2021 with submission ID 1685463685 and the similarity index was found to be 6 %. The complete report running into 28 Pages, 5196 Word count with File Size 2949 KBis being forwarded to the Research Supervisor/DRC/DRB for review

After excluding 1 Research papers co-authored with the Research Supervisor, as annexed as A-1

Date 27.10.2021

Swami Vivekananda Library and Resource Centre ★ Manav Rachna University ★ Faridabad
Rajesh Kumar
27/10/21

27/10/21.

The complete report of the above Short ✓ Synopsis/~~Thesis~~ has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short ✓ Synopsis/~~Thesis~~ may be considered for further processing

Barkhashree 27/10/2021
Research Scholar

27/10/21
Research Supervisor

Barkhashree Short Synopsis 27.10.2021

by Barkhashree D

Submission date: 27-Oct-2021 02:42PM (UTC+0530)
Submission ID: 1685463685
File name: A_PARADIGM_SHIFT_Barkhashree_Short_Synopsis_27.10.2021.docx (86.11K)
Word count: 5196
Character count: 33138

A PARADIGM SHIFT TO OPTIMIZE THE DIGITAL FORENSICS PROCESS

SHORT SYNOPSIS

by

Barkhashree
2K19-PFE-004

Under the supervision of

Dr. Parneeta Dhaliwal
Professor

Department of Computer Science and Technology
Faculty of Engineering

Barkhashree Short Synopsis 27.10.2021

ORIGINALITY REPORT

Excluding matches less than 14 words

After excluding 4 Research papers co-authored with the Research Supervisor, as annexed as A

27/10/21

6%	5%	5%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

Rajesh Kumar 27/10

Barkhashree 27/10/2021

PRIMARY SOURCES

1	clok.uclan.ac.uk Internet Source	2%
2	hdl.handle.net Internet Source	1%
3	Asha Asha, Dr. Balkishan. "Systematic Review on the Suspicious Profiles Detection on Online Social Media Data", Oriental journal of computer science and technology, 2017 Publication	<1%
4	Submitted to University of Bedfordshire Student Paper	<1%
5	www.researchgate.net Internet Source	<1%
6	Submitted to Rajarambapu Institute of Technology Student Paper	<1%
7	Submitted to Study Group Australia Student Paper	<1%
8	eprints.staffs.ac.uk Internet Source	<1%

9	www.ejournal.aessangli.in Internet Source	<1%

Exclude quotes	On	Exclude matches	< 14 words
Exclude bibliography	On		

Annexure A

Parneeta 27/10/21.

International Journal of Digital Crime and Forensics
Volume 13 • Issue 5 • September-October 2021

Behavioural Evidence Analysis: A Paradigm Shift in Digital Forensics

Barkha Shree, Manav Rachna University, Faridabad, India
Parneeta Dhaliwal, Manav Rachna University, Faridabad, India

ABSTRACT

Recent developments in digital forensics (DF) have emphasized that along with inspection of digital evidence, the study of behavioural clues based on behavioural evidence analysis (BEA) is vital for accurate and complete criminal investigation. This paper reviews the existing BEA approaches and process models and concludes the lack of standardisation in the BEA process. The research comprehends that existing BEA methodologies are restricted to specific characteristics of the forensic domain in question. To address these limitations, the paper proposes a standardised approach detailing the step-by-step implementation of BEA in the DF process. The proposed model presents a homogenous technique that can be practically applied to real-life cases. This standard BEA framework classifies digital evidence into categories to decipher associated offender characteristics. Unlike existing models, this new approach collects evidence from diverse sources and leaves no aspect unattended while probing criminal behavioural cues, thus facilitating its applicability across varied forensic domains.

KEYWORDS

BEA, Behavioural Analysis, Behavioural Evidence Analysis, Criminal Profiling, Digital Evidence, Digital Forensics, Forensic Analysis

INTRODUCTION

The role of technology is ever-increasing in today's world. The inception of technology has provided some unique opportunities (Sedera & Cooper, 2019) towards creating a modern society but it can also be abused and misused by individuals. The plethora of tools and technologies (Dawson & Omar, 2015) available today that allow criminal acts to occur anywhere in the world serve as an incentive for criminals. The offenses carried out by criminals facilitated by a computer (McMurdie, 2016), computer networks or any other type of information communications technology are known as Digital crimes. It also involves classic crimes (such as murder, blackmailing, kidnaping, defamation), that misuse technological adeptness and accessibility to information. Formerly, criminal investigations revolved around the analysis of physical evidence from the crime scene. Whereas today, in the digital era, the evidence to assay is in an electronic or digital form (Macdermott, Baker, & Shi, 2018) and is called Digital Evidence. Digital evidence is any information related to the crime that is stored or transmitted in digital form. It may comprise of computer-generated log files, browsing history, or metadata and may be accrued from computer systems, smart digital devices, or network traffic.

The mechanism required to obtain and analyze digital evidence to solve criminal cases is called Digital Forensics (Årnes, 2017; Sammons, 2015). It is a new and fast-growing form of investigative

DOI: 10.4018/IJDCF.20210901.oa2

This article, published as an Open Access article on July 2nd, 2021 in the gold Open Access journal, theInternational Journal of Digital Crime and Forensics (converted to gold Open Access January 1st, 2021), is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.